Kropp Exhibit A

[Redacted]

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
SEATTLE DIVISION

KAELI GARNER, *et al.*, Plaintiffs, v. AMAZON.COM, INC., a Delaware Corporation, and AMAZON.COM SERVICES LLC, a Delaware Limited Liability Company, Defendants.	Case No. 2:21-cv-00750-RSL

EXPERT REPORT OF SERGE EGELMAN, Ph.D.

June 18, 2024

TABLE OF CONTENTS

I. INTRODUCTION

1. I, Serge Egelman, was asked to provide an expert opinion in the matter of *Garner et al v. Amazon.com Inc et al (No. 2:2021-cv-00750)*. In the remainder of this section, I provide information about my background and experience.

2. I am the Research Director of the Usable Security and Privacy group at the International Computer Science Institute (ICSI), which is an independent research institute affiliated with the University of California, Berkeley. I also hold a position as a research scientist within the Electrical Engineering and Computer Sciences (EECS) Department at the University of California, Berkeley. I am also a co-founder and Chief Scientist of AppCensus, Inc., which is a company that was spun off of my academic research that builds tools to test the privacy behaviors of mobile apps. I received my Ph.D. from Carnegie Mellon University's School of Computer Science. My research has been cited over 13,000 times,[1] and my h-index—the most common metric for scientific impact—is over 50.[2]

3. I have been performing research into online privacy for nearly twenty years. My research focuses on the interplay of online privacy, computer security, and human factors. In short, I study: consumer privacy and security decision making; consumer privacy preferences; privacy and security expectations; and how those expectations comport with reality (e.g., by performing technical analyses of online services and other software to examine privacy and security practices). This research involves both technical knowledge to build tools for use in measurement studies (e.g., observational studies of how user data is

[1] Profile of Serge Egelman, Google Scholar, https://scholar.google.com/citations?user=WN9t4n0AAAAJ&hl=en
[2] *See* Curriculum Vitae attached as Appendix A.

collected and shared in practice), as well as a deep understanding of how to apply social science methodologies (e.g., human subjects research, surveys, interviews, randomized controlled trials, etc.). I have served as an invited expert for several web standards efforts that pertained to privacy and security, and have received over a dozen awards from the research community (including: privacy research awards from two European data protection authorities, AEPD in Spain and CNIL in France; the USENIX Security Symposium Distinguished Paper Award, from one of the top academic computer security conferences; the Caspar Bowden Award for Outstanding Research in Privacy Enhancing Technologies; and seven paper awards from the ACM Special Interest Group on Computer-Human Interaction [SIGCHI], the top human-computer interaction conference). I have also been repeatedly invited to speak at the FTC's annual "PrivacyCon" event based on my laboratory's research.

4. Based on my research, I am also regularly asked to consult for regulatory authorities on privacy issues (e.g., the FTC and various state attorneys general); I have also testified before the U.S. Senate based on my research. Based on commercial demand for the tools that my lab developed and the data that they produce, I co-founded a company, AppCensus, Inc., which is commercializing my academic research by performing on-demand privacy analysis of mobile apps to help developers comply with regulatory requirements, and to help regulators and watchdog groups (e.g., journalists and non-profits) verify compliance. I have also specifically performed several research studies on consumers' understandings and expectations concerning data captured from within the home by Internet-connected devices, which has included supervising multiple

dissertations on the topic. My qualifications are described more thoroughly in my curriculum vitae, which appears at the end of this report.

5. Plaintiffs' Counsel are paying my rate of $600 per hour for my services. My compensation is in no way contingent on the outcome of this case. In this report, I was asked to examine several documents about how Amazon's Alexa service works and internal communications amongst Amazon's employees. I examined what information was collected by the service (e.g., sensitive and personally identifiable user information), under what circumstances, and how it was used.

6. The materials I have considered when forming my opinions are cited herein as footnotes. It is my understanding that the Defendants precluded me from reviewing certain relevant documents. I reserve the right to amend this report, including to reflect new information that becomes available to me in light of the discovery process and/or further rulings from the Court.

II. SUMMARY OF OPINIONS

7. Based on my knowledge, expertise, and experience, the documents shared with me, and prior published research, I have formed the following opinions:

    a) Amazon's Alexa service intercepts audio recorded within homes and transmits it to Amazon's servers. This interception and transmission occurs in real time. It is clear to me that devices using Amazon's Alexa service may intercept audio and transmit it to Amazon's servers when the Alexa service should not do so. That is, audio is recorded and transmitted even when users have not asked Alexa to listen to their speech (i.e., when speaking the "wake word,") (§ IV).

b) Audio that was not intended for Alexa was recorded, transmitted, and collected, and should have been discarded when Amazon discovered that no "wake word" was present, but instead the audio was used by Amazon for its own purposes. Amazon was aware that it recorded, collected, and stored audio and related data in defiance of its customers' reasonable expectations, and that this was creating a privacy problem for Amazon (§ V).

c) Humans hired by Amazon listened to some of the audio not intended for Alexa and Amazon believed that these individuals may have accessed and copied these recordings inappropriately.

d) The audio recordings Amazon intercepted, transmitted, and (in some cases) made available to humans, often include voice recordings, which are personally identifiable (§ V).

e) Amazon compensated some individuals to use their audio recordings for Amazon's research and development purposes. However, to save money, Amazon also collected, used, and benefited from billions of audio recordings collected from people without their consent. In certain instances, individuals had no idea that any of this audio capture was occurring, and thus had no opportunity to reasonably opt out of it (§§ V–VI).

f) Based on my prior research, it is clear to me that consumers would have found these practices objectionable. Consumers view audio captured within their homes as highly-sensitive and private (§§ VI–VII). This type of data—voice recordings—is personally identifiable (§ VIII).

III. HOW ALEXA WORKS

8. Alexa is a "virtual personal assistant" developed by Amazon.[3] The service allows consumers to use their voices to speak commands or queries. For example, commands might include requesting that Alexa control other Internet-connected devices (e.g., turning smart light switches on or off); queries might include asking Alexa to search the Internet for certain information (e.g., finding a recipe or the weather forecast). On some devices, voice assistants can be activated and instructed to start listening by pressing a button, akin to the "listen" button that many cars have on their steering wheels.

9. However, when Amazon Alexa was first introduced, as the voice assistant for the Amazon Echo smart speaker, users could activate it by speaking its "wake word,"[4] "Alexa." The Amazon Echo and its successors "use on-device technology to detect when the wake word is spoken and then turn on the audio stream to the Alexa system in the cloud."[5]

10. "The cloud" is a term of art for remote servers, popularized in part by the introduction of Amazon Web Services. In this case, it means computers that are owned and operated by Amazon, which reside in data centers around the world.

11. Alexa-enabled devices must constantly record[6] data from their microphones and analyze data locally (on the device) to detect the "wake word" when it is spoken.

12. [redacted]

[3] *See* Curriculum Vitae.
[4] Ipsic, I. (Ed.). (2011). Speech Technologies. InTech. doi: 10.5772/669.
[5] AMZ_GARNER_00048010.
[6] Even if storing that data for a matter of milliseconds.

[redacted]

13. [redacted]

14. [redacted]

[7] AMZ_GARNER_00054156; AMZ_GARNER_00054157.
[8] Ipsic, I. (Ed.). (2011). Speech Technologies. InTech. doi: 10.5772/669.
[9] AMZ_GARNER_00048007.
[10] AMZ_GARNER_00057114 at 2.
[11] AMZ_GARNER_00048008; AMZ_GARNER_01221121 at 3; AMZ_GARNER_02031348.
[12] AMZ_GARNER_00337109.

15. [redacted]

16. [redacted]

IV. AUDIO IS INAPPROPRIATELY RECORDED AND SENT TO AMAZON

17. [redacted]

[13] *Id.*
[14] *Id.* at '7112.
[15] *Id.* at '7111.
[16] AMZ_GARNER_00048008; AMZ_GARNER_01221121 at 20.
[17] AMZ_GARNER_00052923.

[redacted]

18. [redacted]

19. [redacted]

[18] AMZ_GARNER_00048010.
[19] AMZ_GARNER_00048011.
[20] AMZ_GARNER_00052921 at '2922.
[21] *Id.*
[22] AMZ_GARNER_00098033.

[redacted]

20. [redacted]

21. [redacted]

22. [redacted]

[23] *Id.*
[24] AMZ_GARNER_00856790.
[25] AMZ_GARNER_00337109.
[26] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, David Wagner, and Serge Egelman. Privacy Attitudes of Smart Speaker Users. Proceedings on Privacy Enhancing Technologies (PoPETS), 2019(4).
[27] AMZ_GARNER_00428244.

23. [redacted]

24. [redacted]

[28] AMZ_GARNER_00188334.
[29] AMZ_GARNER_01107376.
[30] AMZ_GARNER_01271023.
[31] AMZ_GARNER_00931443.

25. [redacted]

V. AMAZON BENEFITS FROM INAPPROPRIATELY-COLLECTED AUDIO

26. Data that is collected through people's use of Alexa is used by Amazon for its own purposes: "Amazon uses your requests to Alexa to train our speech recognition and natural language understanding systems using machine learning. Training Alexa with real world requests from a diverse range of customers is necessary for Alexa to respond properly to the variation in our customers' speech patterns, dialects, accents, and vocabulary and the acoustic environments where customers use Alexa. This training relies in part on supervised machine learning, an industry-standard practice where humans review an extremely small sample of requests to help Alexa understand the correct interpretation of a request and provide the appropriate response in the future. For example, a human reviewing a customer's request for the weather in Austin can identify that Alexa misinterpreted it as a request for the weather in Boston."[34]

27. While collecting customer data to train and improve machine learning models is an industry standard practice, it is incumbent on the collector to ensure customers are

[32] AMZ_GARNER_00856790.
[33] AMZ_GARNER_01641430.
[34] AMZ_GARNER_00048007 at AMZ_GARNER_00048012 (Amazon's privacy and data handling document).

informed and consent to the collection of the data and how it may be used (*e.g.*, that it may be shared with human employees/contractors who will listen to it)—which Amazon failed to do here. In any case, individuals that did not register Alexa devices or accounts could not consent. Prior research on data captured from "bystanders" (*i.e.,* those in proximity of the device who have their data collected, even though they are not users of the device nor have they otherwise consented to data capture; *e.g.,* house guests, in-home medical providers, childcare professionals, etc.) has shown that these individuals strenuously object to their data being captured without their consent or awareness.[35] "Participants expressed interest in being asked permission before being recorded and in recording-blocking devices."[36]

28. [redacted]

[35] *E.g.,* Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. Proc. ACM Hum.-Comput. Interact. 3, CSCW, Article 59 (November 2019), 24 pages; Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühlhäuser. 2020. "I don't know how to protect myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments. In Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society (NordiCHI '20). Association for Computing Machinery, New York, NY, USA, Article 4, 1–11; Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. In situ with bystanders of augmented reality glasses: perspectives on recording and privacy-mediating technologies. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14). Association for Computing Machinery, New York, NY, USA, 2377–2386; Bernd, J., Abu-Salma, R., & Frik, A. (2020). Bystanders' Privacy: The Perspectives of Nannies on Smart Home Surveillance. In 10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20); Maximiliane Windl and Sven Mayer. 2022. The Skewed Privacy Concerns of Bystanders in Smart Environments. Proc. ACM Hum.-Comput. Interact. 6, MHCI, Article 184 (September 2022), 21 pages; Yue Huang, Borke Obada-Obieh, and Konstantin (Kosta) Beznosov. 2020. Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20). Association for Computing Machinery, New York, NY, USA, 1–13; Bernd, Julia, Ruba Abu-Salma, Junghyun Choy, and Alisa Frik. "Balancing power dynamics in smart homes: Nannies' perspectives on how cameras reflect and affect relationships." In Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022), pp. 687-706. 2022; Ahmed Alshehri, Joseph Spielman, Amiya Prasad, and Chuan Yue. 2022. Exploring the Privacy Concerns of Bystanders in Smart Homes from the Perspectives of both Owners and Bystanders. In Proceedings on Privacy Enhancing Technologies. 99–119.

[36] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. In situ with bystanders of augmented reality glasses: perspectives on recording and privacy-mediating technologies. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14). Association for Computing Machinery, New York, NY, USA, 2377–2386.

29. [redacted]

[37] AMZ_GARNER_00386864.
[38] AMZ_GARNER_01271023.
[39] What is Supervised Learning?, https://cloud.google.com/discover/what-is-supervised-learning

30. [redacted]

31. [redacted]

32. [redacted]

33. [redacted]

[redacted]

[40] AMZ_GARNER_01848007 – AMZ_GARNER_01848008.
[41] AMZ_GARNER_01271023.
[42] AMZ_GARNER_00490113–00490114; AMZ_GARNER_00634867.
[43] AMZ_GARNER_02031353.
[44] AMZ_GARNER_03203468.

[redacted]

34. [redacted]

35. [redacted]

VI. THE PUBLIC IS LIKELY UNAWARE AUDIO WAS COLLECTED

36. [redacted]

[45] AMZ_GARNER_03203468 at 3474.
[46] AMZ_GARNER_00581214.
[47] AMZ_GARNER_02913152; "en-US" refers to English-speaking US users.
[48] AMZ_GARNER_02913150.
[49] AMZ_GARNER_00048013.
[50] AMZ_GARNER_00054957.

[redacted]

37. These findings are consistent with research performed by others: "[m]ost participants mentioned a lack of knowledge of what is happening with their data and that they were not given a chance to give informed consent. Some participants felt that it is the provider's responsibility to ensure that information on data collection and use is understood by their users and that they have failed to be transparent enough. [An anonymous participant] explained that 'Amazon should make people aware of how and

[51] *E.g.,* Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020. "You just can't know about everything": Privacy Perceptions of Smart Home Visitors. In Proceedings of the 19th International Conference on Mobile and Ubiquitous Multimedia (MUM '20). Association for Computing Machinery, New York, N.Y, 83–95; ("the visitors of smart environments demonstrated similar privacy preferences like the owners of IoT devices but lacked means to judge consequences of data collection and means to express their privacy preferences").
[52] AMZ_GARNER_00337079.
[53] AMZ_GARNER_00048014.
[54] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, David Wagner, and Serge Egelman. Privacy Attitudes of Smart Speaker Users. Proceedings on Privacy Enhancing Technologies (PoPETS), 2019(4).
[55] *Id.*

who and what data they are collecting' to allow people to make an informed decision of whether to use their service."[56]

38. [redacted]

39. [redacted]

40. [redacted]

VII. PEOPLE CONSIDER IN-HOME AUDIO RECORDINGS TO BE HIGHLY SENSITIVE

41. [redacted]

[56] Nicole Meng, Dilara Keküllüoğlu, and Kami Vaniea. 2021. Owning and Sharing: Privacy Perceptions of Smart Speaker Users. Proc. ACM Hum.-Comput. Interact. 5, CSCW1, Article 45 (April 2021), 29 pages.
[57] AMZ_GARNER_00048014.
[58] AMZ_GARNER_00323704.
[59] Li Li, Yuxi Fan, Mike Tse, Kuo-Yi Lin. "A review of applications in federated learning," *Computers & Industrial Engineering*, Vol. 149, Nov. 2020, https://doi.org/10.1016/j.cie.2020.106854.
[60] AMZ_GARNER_00323704.
[61] AMZ_GARNER_00395113.
[62] AMZ_GARNER_00395116.
[63] AMZ_GARNER_01012801.

42. My peer-reviewed research has documented consumers' concerns about inappropriate voice recordings. In a 2012 publication,[64] colleagues and I surveyed 3,115 consumers about data collection risks associated with using smartphone apps. For each risk, participants chose an answer from a 5-point scale that ranged from "Indifferent" to "Very upset." Among those risks, we asked how they would feel if an app "recorded you speaking with your phone's microphone." We asked each participant about a randomly-selected subset of 12 of the 99 risks we were investigating, yielding approximately 377 responses for each risk. Of those asked how they would feel if an app "recorded you speaking with your phone's microphone," 79% responded that they would be "very upset."[65]

43. In a follow-up peer-reviewed survey in 2016, colleagues and I examined consumers' reactions to unexpected data capture by wearable Internet-connected devices.[66] This included examining how the percentage of participants who would be very upset by non-consensual audio recordings would vary depending on what was being recorded. The percent who were very upset by non-consensual recording ranged from 60%, when recording "sound around you" (background noise) to 86% when recording "work conversations."

44. The 2016 study also showed that people are more likely to be very upset when inappropriately-captured data is shared with humans, as opposed to merely processed by

[64] Adrienne Porter Felt, Serge Egelman, and David Wagner. 2012. *I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns*. In Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices (SPSM '12). https://blues.cs.berkeley.edu/wp-content/uploads/2014/07/spsm12.pdf

[65] *Id.*

[66] Linda Lee, JoongHwa Lee, Serge Egelman, and David Wagner. Information Disclosure Concerns in The Age of Wearable Computing. In Proceedings of the NDSS Workshop on Usable Security (USEC '16). See Table VII. https://blues.cs.berkeley.edu/wp-content/uploads/2016/02/camera-ready.pdf,

machines.[67] "A statistically significant difference in VUR [the percent of participants who reported that they would be very upset] exists between data shared with an application versus human recipients. On average, 42% of participants stated that they would be "very upset" if their data was shared with only an application's servers, whereas the VURs for friends (70%), work contacts (75%), and the public (72%) were almost double (Table II).[68]

45. In another study specifically on in-home virtual assistants, similar to Amazon's Alexa,[69] we asked participants about their level of concern for having an always-listening device in their homes.[70] "Slightly more than half of the time (52.8%), participants were uncomfortable sharing [in-home audio captured by an always-listening device] to receive a service."[71] "Almost 3 in 4 participants (n = 129, 72.5%) mentioned privacy-related aspects playing a role in their preferences. This led 38 participants (21.4%) to decline the services. For example, P104 said: '[It is] encroaching on privacy to an insane degree. Some things are meant to stay private. Always-listening? Are you kidding me?' In addition to the intrusiveness of the device in general, participants were concerned with the invasive or private nature of specific services (n = 19, 10.7%) and sensitivity of the recorded conversations (n = 21, 11.8%)."[72]

46. Finally, in another peer-reviewed study on consumers' expectations about data processing associated with smart TVs (*i.e.*, another example of an in-home Internet-connected device

[67] *Id.*
[68] *Id.* at § III.
[69] In the study, we specifically framed the questions around a generic device, though our description could very well apply to Amazon's Alexa.
[70] Madiha Tabassum, Tomasz Kosiński, Alisa Frik, Nathan Malkin, Primal Wijesekera, Serge Egelman, and Heather Richter Lipford. 2020. Investigating Users' Preferences and Expectations for Always-Listening Voice Assistants. Proc. ACM Interact. Mob. Wearable Ubiquitous Tech.. 3, 4, Article 153 (Dec. 2019), 23 pages.
[71] *Id.*
[72] *Id.*

that has the ability to exfiltrate personally-identifiable information from within the home), we asked several questions about in-home audio capture that could be used for various voice recognition features.[73] We observed that only half of the participants understood that such features require remote processing of their data (*i.e.*, audio recordings would be uploaded to the device manufacturer). Many participants objected to the inappropriate collection of data from within their homes (*e.g.*, if it was discovered that their devices shared data inappropriately) and "73% of respondents predicted they would be less likely to purchase another device from that manufacturer."[74]

VIII. VOICE RECORDINGS ARE PERSONALLY IDENTIFIABLE

47. Voice recordings are inherently personally-identifiable information because the voice identifies the speaker: anyone listening to a voice recording can identify the speaker if they recognize the voice. "No two individuals sound identical because of their vocal tract shapes, larynx sizes, and other different voice production organs. In addition to these physical differences, each individual has his or her own speaking style, pronunciation pattern, choice of vocabulary, and so on. Because of all these factors, one can use voice as a bio-metric in addition to fingerprint and retinal scans."[75]

48. Moreover, one does not need to even know the speaker to recognize their voice: technology allows for voices to be identified and matched, even if the speaker is a complete stranger. Speaker recognition technology has existed since the 1950s and has

[73] N. Malkin, J. Bernd, M. Johnson, S. Egelman. "What can't data Be used for?": privacy expectations about smart TVs in the U.S. Proc. 3rd Euro. Workshop Useable Secur., Internet Society, London, England (Apr. 2018), 10.14722/eurousec.2018.23016.
[74] *Id.*
[75] K.N.R.K. Raju Alluri, and Anil Kumar Vuppala. "Chapter 7 - A study on the emotional state of a speaker in voice bio-metrics." In *Advances in ubiquitous sensing applications for healthcare*, Amy Neustein (ed.), Advances in Ubiquitous Computing, Academic Press, May 2020.

drastically improved over the intervening decades.[76] Commercial products to identify individuals from short snippets of audio are in widespread deployment (i.e., products that are specifically designed to identify an individual from a short voice recording).[77] In many cases, short utterances of 1–2 seconds are sufficient to identify the speaker.[78] This technology will only improve.

49. Voice prints and recordings are widely-known to be personally-identifiable data and are regulated as such. For example, HIPAA § 164.514(b) states that "a covered entity may determine that health information is not individually identifiable health information only if: … (2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:… (P) Biometric identifiers, including finger and voice prints."[79] Under CCPA, audio recordings are similarly considered biometric data[80] and biometric data (including audio) are considered Personal Information.[81]

50. [redacted]

[76] Xiong Xiong. 2023. A Summary of the Development of Speech Recognition Technology. In Proceedings of the 2022 4th International Conference on Robotics, Intelligent Control and Artificial Intelligence (RICAI '22). Association for Computing Machinery, Dec. 2022 New York, NY at 768–773.
[77] *E.g.,* https://docs.nvidia.com/nemo-framework/user-guide/latest/nemotoolkit/asr/speaker_diarization/intro.html; https://azure.microsoft.com/en-us/products/ai-services/speaker-recognition.
[78] Kye, Seong Min, Youngmoon Jung, Hae Beom Lee, Sung Ju Hwang, and Hoirin Kim. "Meta-Learning for Short Utterance Speaker Recognition with Imbalance Length Pairs." InterSpeech 2020.
[79] While Amazon's Alexa service is obviously not a covered entity under HIPAA, my point is simply to show that voice recordings are nearly always considered identifiable-data and various laws explicitly categorize them as such.
[80] Cal. Civ. Code § 1798.140(c).
[81] Cal. Civ. Code §§ 1798.140(v)(1)(E) and 1798.140(v)(1)(H).
[82] AMZ_GARNER_01848005.

51. In the regular course of my research, I must seek approval from my institution's "Institutional Review Board" (IRB) when performing human subjects experiments. In my career I have interacted with many different IRBs at the various institutions with which I have been affiliated, as well as the IRBs at colleagues' institutions. In every case, the IRB considered the collection of voice recordings to be personally-identifiable data (and therefore cannot be considered anonymous or deidentified). For example, noting the identifiability of voice data, the IRBs at UC Berkeley,[83] where I currently work, and the University of Washington,[84] in Defendants' home state (and presumably from which they recruit a significant number of engineers) both consider voice recordings to be personally identifiable and require that the subjects consent prior to recording them. "Information is identifiable when (1) it can be linked to specific individuals, or (2) a combination of the information/characteristics could allow others to ascertain the identities of individuals. Examples of directly identifiable information may include (but are not limited to):…Voice (e.g., audio recording)."[85]

IX. CONCLUSION

52. Based on my twenty years of experience performing peer-reviewed research on data privacy issues, my examination of the documents I reviewed, my education and training, as well as relevant research in the area, it is my expert opinion that: (A) Amazon transmitted audio captured contemporaneously from consumers' homes that was falsely determined to have been preceded by the wake word "Alexa," when in fact no wake word

[83] General Frequently Asked Questions, Berkeley Human Research Protection Program, https://cphs.berkeley.edu/faqs.html#protocol6 ("What constitutes 'identifiable information'?").
[84] "Washington State Law and Consent", University of Washinton Human Subjects Division, https://www.washington.edu/research/hsd/guidance/consent/#audio (which, in turn, cites Revised Code of Washington (RCW) 9.73.030).
[85] General Frequently Asked Questions, Berkeley Human Research Protection Program, https://cphs.berkeley.edu/faqs.html.

was present; (B) Amazon failed to immediately delete said recordings upon determining no wake word was present and no consent to record had been given; (C) that these recordings constitute personally-identifiable information; (D) that Amazon then used those recordings to its commercial benefit; and (E) those uses included the sharing of those recordings with employees and contractors (humans), which consumers find to be a particularly egregious misuse of non-consensually recorded audio.

53. While Amazon could have accomplished the same goal using consenting participants, it opted not to as a cost-saving measure, despite the privacy concerns that employees repeatedly raised over several years.

I declare under penalty of perjury under the laws of the State of Washington and the United States that the foregoing is true and correct.

Executed on this 18th day of June, 2024 in Berkeley, CA.

Serge Egelman, Ph.D.

Research Director, Usable Security and Privacy
International Computer Science Institute (ICSI)

Research Scientist, Electrical Engineering and Computer Sciences (EECS)
University of California, Berkeley

Co-Founder and Chief Scientist
AppCensus, Inc.

Appendix A

SergeEgelman

contact
2150 Shattuck Avenue
Suite 250
Berkeley, CA 94704
USA

egelman@cs.berkeley.edu

education

2009	**PhD** in Computation, Organizations, and Society School of Computer Science	Carnegie Mellon University
2004	**BS** in Computer Engineering School of Engineering and Applied Science	University of Virginia

experience

	AppCensus, Inc.	San Francisco, CA
2022–Now	Chief Scientist / Co-Founder	
2019–2022	CTO / Co-Founder	
	International Computer Science Institute	Berkeley, California
2016–Now	Research Director, Usable Security & Privacy Group	
2013–2016	Senior Researcher, Networking and Security Group	
	University of California, Berkeley	Berkeley, California
2011–Now	Research Scientist, Electrical Engineering and Computer Sciences	
	National Institute of Standards and Technology	Gaithersburg, Maryland
2010–2011	Research Scientist, Visualization and Usability Group	
	Brown University	Providence, Rhode Island
2009-2010	Postdoctoral Researcher, Computer Science Department	
	Microsoft Research	Redmond, Washington
2008	Research Intern, Security and Privacy Group	
2008	Research Intern, VIBE Group	
	PARC	Palo Alto, California
2006	Research Intern, Computer Science Laboratory	

publications*

refereed journal publications

A Model of Contextual Factors Affecting Older Adults' Information-Sharing Decisions in the U.S.
Frik, A., Bernd, J., and Egelman, S. ACM Transactions on Computer-Human Interaction *30.1 (Apr. 2023). Association for Computing Machinery.*

Lessons in VCR Repair: Compliance of Android App Developers with the California Consumer Privacy Act (CCPA)

*Over 12,000 citations and h-index=52: https://scholar.google.com/citations?hl=en&user=WN9t4n0AAAAJ

Samarin, N., Kothari, S., Siyed, Z., Bjorkman, O., Yuan, R., Wijesekera, P., Alomar, N., Fischer, J., Hoofnagle, C., and Egelman, S. Proceedings on Privacy Enhancing Technologies (PoPETS) *3 (2023).*

Developers Say the Darnedest Things: Privacy Compliance Processes Followed by Developers of Child-Directed Apps
Alomar, N., and Egelman, S. Proceedings on Privacy Enhancing Technologies (PoPETS) *4 (2022) pp. 250–273.*

Data Collection Practices of Mobile Applications Played by Preschool-Aged Children
Zhao, F., Egelman, S., Weeks, H. M., Kaciroti, N., Miller, A. L., and Radesky, J. S. JAMA Pediatrics *174.12 (Dec. 2020).*

Nudge Me Right: Personalizing Online Security Nudges to People's Decision-Making Styles
Peer, E., Egelman, S., Harbach, M., Malkin, N., Mathur, A., and Frik, A. Computers in Human Behavior *109 (Aug. 2020).*

Disaster Privacy/Privacy Disaster
Sanfilippo, M. R., Shvartzshnaider, Y., Reyes, I., Nissenbaum, H., and Egelman, S. Journal of the Association for Information Science and Technology *(Mar. 2020).*

Can You Pay For Privacy? Consumer Expectations and the Behavior of Free and Paid Apps
Bamberger, K. A., Egelman, S., Han, C., Elazari, A., and Reyes, I. Berkeley Technology Law Journal *35 (2020).*

The Price is (Not) Right: Comparing Privacy in Free and Paid Apps
Han, C., Reyes, I., Feal, Á., Reardon, J., Wijesekera, P., Vallina-Rodriguez, N., Elazari, A., Bamberger, K. A., and Egelman, S. Proceedings on Privacy Enhancing Technologies (PoPETS) *3 (2020).*

Investigating Users' Preferences and Expectations for Always-Listening Voice Assistants
Tabassum, M., Kosiński, T., Frik, A., Malkin, N., Wijesekera, P., Egelman, S., and Lipford, H. R. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technoligies (IMWUT) *3.4 (Dec. 2019). Association for Computing Machinery.*

Privacy Attitudes of Smart Speaker Users
Malkin, N., Deatrick, J., Tong, A., Wijesekera, P., Wagner, D., and Egelman, S. Proceedings on Privacy Enhancing Technologies *2019.4 (2019).*

"Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale
Reyes, I., Wijesekera, P., Reardon, J., On, A. E. B., Razaghpanah, A., Vallina-Rodriguez, N., and Egelman, S. Proceedings on Privacy Enhancing Technologies *2018.3 (2018) pp. 63–83.* **Caspar Bowden PET Award**

A Usability Evaluation of Tor Launcher
Lee, L., Fifield, D., Malkin, N., Iyer, G., Egelman, S., and Wagner, D. Proceedings on Privacy Enhancing Technologies *2017.3 (2017) pp. 87–106.*

The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study
Tsai, J., Egelman, S., Cranor, L., and Acquisti, A. Information Systems Research *22.2 (2011) pp. 254–268.* **AIS Best Publication of 2011 Award / INFORMS Best Published Paper Award (2012)**

P3P Deployment on Websites
Cranor, L. F., Egelman, S., Sheng, S., McDonald, A. M., and Chowdhury, A. Electronic Commerce Research and Applications *7.3 (2008) pp. 274–293.*

The Real ID Act: Fixing Identity Documents with Duct Tape
Egelman, S., and Cranor, L. F. I/S: A Journal of Law and Policy for the Information Society *2.1 (2006) pp. 149–183.*

refereed conference publications

Security and Privacy Failures in Popular 2FA Apps
Gilsenan, C., Shakir, F., Alomar, N., and Egelman, S. Proceedings of the 32nd USENIX Security Symposium *(USENIX Security '23), 2023.*

In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes

Girish, A., Hu, T., Prakash, V., Dubois, D. J., Matic, S., Huang, D. Y., Egelman, S., Reardon, J., Tapiador, J., Choffnes, D., and Vallina-Rodriguez, N. Proceedings of the 2023 ACM on Internet Measurement Conference *(IMC '23), 2023, New York, NY, USA.*

Log: It's Big, It's Heavy, It's Filled with Personal Data!
Measuring the Logging of Sensitive Information in the Android Ecosystem
Lyons, A., Gamba, J., Shawaga, A., Reardon, J., Tapiador, J., Egelman, S., and Vallina-Rodriguez, N. Proceedings of the 32nd USENIX Security Symposium *(USENIX Security '23), 2023.*

Can Humans Detect Malicious Always-Listening Assistants?
A Framework for Crowdsourcing Test Drives
Malkin, N., Wagner, D., and Egelman, S. Proceedings of the ACM Conference On Computer-Supported Cooperative Work And Social Computing *(CSCW '22), 2022, New York, NY, USA.*

Runtime Permissions for Privacy in Proactive Intelligent Assistants
Malkin, N., Wagner, D., and Egelman, S. Eighteenth Symposium on Usable Privacy and Security *(SOUPS 2022), 2022.*

"You've Got Your Nice List of Bugs, Now What?" Vulnerability Discovery and Management Processes in the Wild
Alomar, N., Wijesekera, P., Qiu, E., and Egelman, S. Proceedings of the Sixteenth Symposium on Usable Privacy and Security *(SOUPS 2020), 2020.*

Actions Speak Louder than Words: Entity-Sensitive Privacy Policy and Data Flow Analysis with PoliCheck
Andow, B., Mahmud, S. Y., Whitaker, J., Enck, W., Reaves, B., Singh, K., and Egelman, S. 29th USENIX Security Symposium *(USENIX Security '20), 2020, Boston, MA.*

Don't Accept Candies from Strangers: An Analysis of Third-Party Mobile SDKs
Feal, Á., Gamba, J., Tapiador, J., Wijesekera, P., Reardon, J., Egelman, S., and Vallina-Rodriguez, N. International Conference on Computers, Privacy and Data Protection *(CPDP '20), 2020.*

A Qualitative Model of Older Adults' Contextual Decision-Making About Information Sharing
Frik, A., Bernd, J., Alomar, N., and Egelman, S. Workshop on the Economics of Information Security *(WEIS '20), 2020.*

Empirical Measurement of Systemic 2FA Usability
Reynolds, J., Samarin, N., Barnes, J., Judd, T., Mason, J., Bailey, M., and Egelman, S. Proceedings of the 29th USENIX Security Symposium *(USENIX Security '20), 2020.*

A Promise Is A Promise: The Effect of Commitment Devices on Computer Security Intentions
Frik, A., Malkin, N., Harbach, M., Peer, E., and Egelman, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '19), 2019.*

Privacy and Security Threat Models and Mitigation Strategies of Older Adults
Frik, A., Nurgalieva, L., Bernd, J., Lee, J. S., Schaub, F., and Egelman, S. Proceedings of the 15th Symposium on Usable Privacy and Security *(SOUPS '19), 2019, Berkeley, CA, USA.*

Information Design in An Aged Care Context
Nurgalieva, L., Frik, A., Ceschel, F., Egelman, S., and Marchese, M. Proceedings of the 13th International Conference on Pervasive Computing Technologies for Healthcare *(PervasiveHealth '19), 2019, New York, NY, USA.*

50 Ways to Leak Your Data:
An Exploration of Apps' Circumvention of the Android Permissions System
Reardon, J., Feal, A., Wijesekera, P., On, A. E. B., Vallina-Rodriguez, N., and Egelman, S. Proceedings of the 24th USENIX Security Symposium *(USENIX Security '19), 2019, Berkeley, CA, USA.* **USENIX Security Distinguished Paper Award / AEPD Emilio Aced Personal Data Protection Research Award / CNIL-INRIA Privacy Award**

An Experience Sampling Study of User Reactions to Browser Warnings in the Field
Reeder, R. W., Felt, A. P., Consolvo, S., Malkin, N., Thompson, C., and Egelman, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '18), 2018.*

Contextualizing Privacy Decisions for Better Prediction (and Protection)

Wijesekera, P., Reardon, J., Reyes, I., Tsai, L., Chen, J.-W., Good, N., Wagner, D., Beznosov, K., and Egelman, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '18), 2018.* **SIGCHI Honorable Mention Award**

Let's go in for a closer look: Observing passwords in their natural habitat
Pearman, S., Thomas, J., Naeini, P. E., Habib, H., Bauer, L., Christin, N., Cranor, L. F., Egelman, S., and Forget, A. Proc. of the ACM SIGSAC Conference on Computer & Communications Security *(CCS '17), 2017, New York, NY, USA.*

Turtle Guard: Helping Android Users Apply Contextual Privacy Preferences
Tsai, L., Wijesekera, P., Reardon, J., Reyes, I., Egelman, S., Wagner, D., Good, N., and Chen, J.-W. Proceedings of the 13th Symposium on Usable Privacy and Security *(SOUPS '17), 2017.*

The Feasibility of Dynamically Granted Permissions:
Aligning Mobile Privacy with User Preferences
Wijesekera, P., Baokar, A., Tsai, L., Reardon, J., Egelman, S., Wagner, D., and Beznosov, K. Proceedings of the 2017 IEEE Symposium on Security and Privacy *(Oakland '17), 2017.*

Do or Do Not, There Is No Try: User Engagement May Not Improve Security Outcomes
Forget, A., Pearman, S., Thomas, J., Acquisti, A., Christin, N., Cranor, L. F., Egelman, S., Harbach, M., and Telang, R. Proc. of the 12th Symposium on Usable Privacy and Security *(SOUPS '16), 2016.*

Behavior Ever Follows Intention? A Validation of the Security Behavior Intentions Scale (SeBIS)
Egelman, S., Harbach, M., and Peer, E. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '16), 2016.* **SIGCHI Honorable Mention Award**

The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens
Harbach, M., Luca, A. D., and Egelman, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '16), 2016.* **SIGCHI Honorable Mention Award**

Keep on Lockin' in the Free World: A Transnational Comparison of Smartphone Locking
Harbach, M., Luca, A. D., Malkin, N., and Egelman, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '16), 2016.* **SIGCHI Honorable Mention Award**

The Teaching Privacy Curriculum
Egelman, S., Bernd, J., Friedland, G., and Garcia, D. Proceedings of the 47th ACM technical symposium on Computer Science Education *(SIGCSE '16), 2016.*

Android Permissions Remystified: A Field Study on Contextual Integrity
Wijesekera, P., Baokar, A., Hosseini, A., Egelman, S., Wagner, D., and Beznosov, K. 24th USENIX Security Symposium *(USENIX Security 15), 2015, Washington, D.C.*

Is This Thing On? Communicating Privacy on Ubiquitous Sensing Platforms
Egelman, S., Kannavara, R., and Chow, R. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '15), 2015, New York, NY, USA.*

Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS)
Egelman, S., and Peer, E. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '15), 2015, New York, NY, USA.* **SIGCHI Honorable Mention Award**

Fingerprinting Web Users through Font Metrics
Fifield, D., and Egelman, S. Proceedings of the 19th international conference on Financial Cryptography and Data Security *(FC'15), 2015.*

Somebody's Watching Me? Assessing the Effectiveness of Webcam Indicator Lights
Portnoff, R., Lee, L., Egelman, S., Mishra, P., Leung, D., and Wagner, D. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '15), 2015, New York, NY, USA.*

Are You Ready to Lock? Understanding User Motivations for Smartphone Locking Behaviors
Egelman, S., Jain, S., Portnoff, R. S., Liao, K., Consolvo, S., and Wagner, D. Proc. of the ACM SIGSAC Conference on Computer & Communications Security *(CCS '14), 2014, New York, NY, USA.*

The Effect of Developer-Specified Explanations for Permission Requests on Smartphone User Behavior
Tan, J., Nguyen, K., Theodorides, M., Negron-Arroyo, H., Thompson, C., Egelman, S., and Wagner,

D. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '14), 2014, Toronto, Canada.*

The Importance of Being Earnest [in Security Warnings]
Egelman, S., and Schechter, S. Proceedings of the 17th international conference on Financial Cryptography and Data Security *(FC'13), 2013, Okinawa, Japan.*

My Profile Is My Password, Verify Me! The Privacy/Convenience Tradeoff of Facebook Connect
Egelman, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '13), 2013, Paris, France.*

Does My Password Go up to Eleven? The Impact of Password Meters on Password Selection
Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K., and Herley, C. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '13), 2013, Paris, France.*

When It's Better to Ask Forgiveness than Get Permission: Attribution Mechanisms for Smartphone Resources
Thompson, C., Johnson, M., Egelman, S., Wagner, D., and King, J. Proceedings of the Ninth Symposium on Usable Privacy and Security *(SOUPS '13), 2013, Newcastle, United Kingdom.*

Android permissions: user attention, comprehension, and behavior
Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., and Wagner, D. Proceedings of the Eighth Symposium on Usable Privacy and Security *(SOUPS '12), 2012, Washington, D.C.* **SOUPS Best Paper Award (2012) / SOUPS Impact Award (2017)**

Facebook and privacy: it's complicated
Johnson, M., Egelman, S., and Bellovin, S. M. Proceedings of the Eighth Symposium on Usable Privacy and Security *(SOUPS '12), 2012, Washington, D.C.*

It's all about the Benjamins: Incentivizing users to ignore security advice
Christin, N., Egelman, S., Vidas, T., and Grossklags, J. Proceedings of the 15th international conference on Financial Cryptography and Data Security *(FC'11), 2011, Gros Islet, St. Lucia.*

Oops, I did it again: mitigating repeated access control errors on facebook
Egelman, S., Oates, A., and Krishnamurthi, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '11), 2011, Vancouver, BC, Canada.*

Of passwords and people: measuring the effect of password-composition policies
Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., Cranor, L. F., and Egelman, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '11), 2011, Vancouver, BC, Canada.* **SIGCHI Honorable Mention Award**

Timing is everything?: the effects of timing and placement of online privacy indicators
Egelman, S., Tsai, J., Cranor, L. F., and Acquisti, A. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '09), 2009, Boston, MA, USA.*

It's No Secret: Measuring the Security and Reliability of Authentication via 'Secret' Questions
Schechter, S., Brush, A. J. B., and Egelman, S. Proceedings of the 2009 IEEE Symposium on Security and Privacy *(Oakland '09), 2009, Los Alamitos, CA, USA.*

It's not what you know, but who you know: a social approach to last-resort authentication
Schechter, S., Egelman, S., and Reeder, R. W. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '09), 2009, Boston, MA, USA.*

Crying wolf: an empirical study of SSL warning effectiveness
Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N., and Cranor, L. F. Proceedings of the 18th USENIX Security Symposium *(SSYM'09), 2009, Montreal, Canada.*

Family accounts: a new paradigm for user accounts within the home environment
Egelman, S., Brush, A. J. B., and Inkpen, K. M. Proceedings of the 2008 ACM Conference on Computer Supported Cooperative Work *(CSCW '08), 2008, San Diego, CA, USA.*

You've Been Warned: An empirical study of the effectiveness of browser phishing warnings
Egelman, S., Cranor, L. F., and Hong, J. CHI '08: Proceeding of The 26th SIGCHI Conference on Human Factors in Computing Systems *(CHI '08), 2008, Florence, Italy.* **SIGCHI Honorable Mention Award**

Phinding Phish: Evaluating Anti-Phishing Tools
Zhang, Y., Egelman, S., Cranor, L. F., and Hong, J. Proceedings of the 14th Annual Network & Distributed System Security Symposium *(NDSS '07), 2007, San Diego, CA.*

Power Strips, Prophylactics, and Privacy, Oh My!
Gideon, J., Egelman, S., Cranor, L., and Acquisti, A. Proceedings of the Second Symposium on Usable Privacy and Security *(SOUPS '06), 2006, Pittsburgh, PA.*

An analysis of P3P-enabled web sites among top-20 search results
Egelman, S., Cranor, L. F., and Chowdhury, A. Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet *(ICEC '06), 2006, Fredericton, New Brunswick, Canada.*

refereed workshop publications

Challenges in Inferring Privacy Properties of Smart Devices:
Towards Scalable Multi-Vantage Point Testing Methods
Girish, A., Prakash, V., Egelman, S., Reardon, J., Tapiador, J., Huang, D. Y., Matic, S., and Vallina-Rodriguez, N. Proceedings of the 3rd International CoNEXT Student Workshop *(CoNEXT-SW '22), 2022, Rome, Italy.*

Identifying and Classifying Third-Party Entities in Natural Language Privacy Policies
Hosseini, M. B., Pragyan, K., Reyes, I., and Egelman, S. Proceedings of the Second Workshop on Privacy in Natural Language Processing *(PrivateNLP '20), 2020.*

Do You Get What You Pay For? Comparing The Privacy Behaviors of Free vs. Paid Apps
Han, C., Reyes, I., On, A. E. B., Reardon, J., Feal, A., Bamberger, K. A., Egelman, S., and Vallina-Rodriguez, N. The Workshop on Technology and Consumer Protection *(ConPro '19), 2019.*

Privacy Controls for Always-Listening Devices
Malkin, N., Egelman, S., and Wagner, D. Proceedings of the New Security Paradigms Workshop *(NSPW '19), 2019, San Carlos, Costa Rica.*

On The Ridiculousness of Notice and Conset: Contradictions in App Privacy Policies
Okoyomon, E., Samarin, N., Wijesekera, P., On, A. E. B., Vallina-Rodriguez, N., Reyes, I., Feal, A., and Egelman, S. The Workshop on Technology and Consumer Protection *(ConPro '19), 2019.*

Better Late(r) than Never: Increasing Cyber-Security Compliance by Reducing Present Bias
Frik, A., Egelman, S., Harbach, M., Malkin, N., and Peer, E. Workshop on the Economics of Information Security *(WEIS '18), 2018.*

"What Can't Data Be Used For?" Privacy Expectations about Smart TVs in the U.S.
Malkin, N., Bernd, J., Johnson, M., and Egelman, S. Proceedings of the European Workshop on Usable Security *(EuroUSEC '18), 2018.*

Personalized Security Messaging: Nudges for Compliance with Browser Warnings
Malkin, N., Mathur, A., Harbach, M., and Egelman, S. Proceedings of the European Workshop on Usable Security *(EuroUSEC '17), 2017.*

"Is Our Children's Apps Learning?" Automatically Detecting COPPA Violations
Reyes, I., Wijesekera, P., Razaghpanah, A., Reardon, J., Vallina-Rodriguez, N., Egelman, S., and Kreibich, C. The Workshop on Technology and Consumer Protection *(ConPro '17), 2017.*

Information Disclosure Concerns in The Age of Wearable Computing
Lee, L. N., Lee, J. H., Egelman, S., and Wagner, D. Proceedings of the NDSS Workshop on Usable Security *(USEC '16), 2016.*

The Myth of the Average User:
Improving Privacy and Security Systems through Individualization
Egelman, S., and Peer, E. Proceedings of the 2015 Workshop on New Security Paradigms *(NSPW '15), 2015, Twente, The Netherlands.*

Teaching Privacy: What Every Student Needs to Know

Friedland, G., Egelman, S., and Garcia, D. Proceedings of the 46th SIGCSE technical symposium on computer science education *(Workshop), 2015.*

U-PriSM 2: The Second Usable Privacy and Security for Mobile Devices Workshop
Chiasson, S., Crawford, H., Egelman, S., and Irani, P. Proc. of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services *(MobileHCI '13), 2013, Munich, Germany.*

Markets for Zero-day Exploits: Ethics and Implications
Egelman, S., Herley, C., and Oorschot, P. C. van Proceedings of the 2013 Workshop on New Security Paradigms Workshop *(NSPW '13), 2013, Banff, Alberta, Canada.*

Choice Architecture and Smartphone Privacy: There's A Price for That
Egelman, S., Felt, A. P., and Wagner, D. The 2012 Workshop on the Economics of Information Security *(WEIS '12), 2012, Berlin, Germany.*

How Good Is Good Enough? The sisyphean struggle for optimal privacy settings
Egelman, S., and Johnson, M. Proceedings of the Reconciling Privacy with Social Media Workshop *(CSCW '12 Workshop), 2012, Seattle, WA.*

It's Not Stealing if You Need It: A Panel on the Ethics of Performing Research Using Public Data of Illicit Origin
Egelman, S., Bonneau, J., Chiasson, S., Dittrich, D., and Schechter, S. Proceedings of the 16th International Conference on Financial Cryptography and Data Security *(FC'12), 2012.*

How to ask for permission
Felt, A. P., Egelman, S., Finifter, M., Akhawe, D., and Wagner, D. Proceedings of the 7th USENIX conference on Hot Topics in Security *(HotSec'12), 2012, Bellevue, WA.*

I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns
Felt, A. P., Egelman, S., and Wagner, D. Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices *(SPSM '12), 2012, Raleigh, North Carolina, USA.*

Toward Privacy Standards Based on Empirical Studies
Egelman, S., and McCallister, E. The Workshop on Web Tracking and User Privacy *(W3C Workshop), 2011, Princeton, NJ.*

Please Continue to Hold: An Empirical Study on User Tolerance of Security Delays
Egelman, S., Molnar, D., Christin, N., Acquisti, A., Herley, C., and Krishnamurthi, S. Workshop on the Economics of Information Security (WEIS '10) *(WEIS '10), 2010, Cambridge, MA.*

Tell Me Lies: A Methodology for Scientifically Rigorous Security User Studies
Egelman, S., Tsai, J., and Cranor, L. F. Proceedings of the Workshop on Studying Online Behavior *(CHI '10 Workshop), 2010, Atlanta, GA.*

This is Your Data on Drugs: Lessons Computer Security Can Learn from the Drug War
Molnar, D., Egelman, S., and Christin, N. Proceedings of the 2010 Workshop on New Security Paradigms *(NSPW '10), 2010, Concord, Massachusetts, USA.*

Security user studies: methodologies and best practices
Egelman, S., King, J., Miller, R. C., Ragouzis, N., and Shehan, E. CHI '07 Extended Abstracts on Human Factors in Computing Systems *(CHI EA '07), 2007, San Jose, CA, USA.*

The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study
Tsai, J., Egelman, S., Cranor, L., and Acquisti, A. Proceedings of the 2007 Workshop on the Economics of Information Security *(WEIS '07), 2007, Pittsburgh, PA, USA.*

Studying the Impact of Privacy Information on Online Purchase Decisions
Egelman, S., Tsai, J., Cranor, L. F., and Acquisti, A. Proceedings of the Workshop on Privacy and HCI: Methodologies for Studying Privacy Issues *(CHI '06 Workshop), 2006, Montreal, Canada.*

book chapters and magazine articles

50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System

Reardon, J., Feal, Á., Wijesekera, P., On, A. E. B., Vallina-Rodriguez, N., and Egelman, S. *;login:* 2019, USENIX Association.

Predicting Privacy and Security Attitudes
Egelman, S., and Peer, E. *Computers and Society*, 2015, ACM.

Crowdsourcing
Egelman, S., Chi, E., and Dow, S. *Ways of Knowing in HCI*, 2013, Springer.

Helping users create better passwords
Ur, B., Kelley, P. G., Komanduri, S., Lee, J., Maass, M., Mazurek, M., Passaro, T., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L. F., Egelman, S., and Lopez, J. *;login:* 2012, USENIX Association.

Suing Spammers for Fun and Profit
Egelman, S. *;login:* 2004, USENIX Association.

Installation
Egelman, S. *Peter Norton's Complete Guide to Linux*, 1999, Macmillan Computer Publishing.

User Administration
Egelman, S. *Peter Norton's Complete Guide to Linux*, 1999, Macmillan Computer Publishing.

awards and recognition

2022 **CNIL-INRIA Privacy Award**
50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System, with J. Reardon, A. Feal, P. Wijesekera, A. Elazari Bar On, and N. Vallina-Rodriguez.

Emilio Aced Personal Data Protection Research Award
50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System, with J. Reardon, A. Feal, P. Wijesekera, A. Elazari Bar On, and N. Vallina-Rodriguez.

2020 **Caspar Bowden Award for Outstanding Research in Privacy Enhancing Technologies**
"Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale, with I. Reyes, P. Wijesekera, J. Reardon, A. Elazari, A. Razaghpanah, and N. Vallina-Rodriguez.

2019 **USENIX Security Symposium Distinguished Paper Award**
50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System, with J. Reardon, A. Feal, P. Wijesekera, A. Elazari Bar On, and N. Vallina-Rodriguez.

2018 **SIGCHI Honorable Mention Award (Best Paper Nominee)**
Contextualizing Privacy Decisions for Better Prediction (and Protection), with P. Wijesekera, J. Reardon, I. Reyes, L. Tsai, J.-W. Chen, N. Good, D. Wagner, and K. Beznosov.

2017 **Symposium on Usable Privacy and Security (SOUPS) Impact Award**
Android Permissions: User Attention, Comprehension, and Behavior, with A. P. Felt, E. Ha, A. Haney, E. Chin, and D. Wagner.

Elected ACM Senior Member Association for Computing Machinery (ACM)

2016 **Symposium on Usable Privacy and Security (SOUPS) Distinguished Poster Award**
Risk Compensation in Home-User Computer Security Behavior: A Mixed-Methods Exploratory Study, with S. Pearman, A. Kumar, N. Munson, C. Sharma, L. Slyper, L. Bauer, and N. Christin.

SIGCHI Honorable Mention Award (Best Paper Nominee)
Behavior Ever Follows Intention? A Validation of the Security Behavior Intentions Scale (SeBIS), with M. Harbach and E. Peer.

SIGCHI Honorable Mention Award (Best Paper Nominee)
The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens, with M. Harbach and A. De Luca.

SIGCHI Honorable Mention Award (Best Paper Nominee)
Keep on Lockin' in the Free World: A Transnational Comparison of Smartphone Locking, with M. Harbach, A. De Luca, and N. Malkin.

2015 **SIGCHI Honorable Mention Award (Best Paper Nominee)**
Scaling the Security Wall: Developing a Security Behavior Intentions Scale, with E. Peer.

2012 **AIS Best Publication of 2011**
The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, with J. Tsai, L. Cranor, and A. Acquisti.

ISR Best Published Paper
The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, with J. Tsai, L. Cranor, and A. Acquisti.

SOUPS Best Paper Award
Android Permissions: User Attention, Comprehension, and Behavior, with A. P. Felt, E. Ha, A. Haney, E. Chin, and D. Wagner.

2011 **SIGCHI Honorable Mention Award (Best Paper Nominee)**
Of Passwords and People: Measuring the Effect of Password-Composition Policies, with S. Komanduri, R. Shay, P. G. Kelley, M. Mazurek, L. Bauer, N. Christin, and L. F. Cranor.

2008 **SIGCHI Honorable Mention Award (Best Paper Nominee)**
You've Been Warned: An Empirical Study on the Effectiveness of Web Browser Phishing Warnings, with L. Cranor and J. Hong.

2006 **Tor Graphical User Interface Design Competition**
Phase 1 Overall Winner, with L. Cranor, J. Hong, P. Kumaraguru, C. Kuo, S. Romanosky, J. Tsai, and K. Vaniea.

Publisher's Clearing House Finalist
I *may* already be a winner.

expert testimony and reports

2024 Expert witness for the plaintiffs in *Clark, et. al. v. Yodlee, Inc., No: 3:20-cv-05991-SK (N.D. Cal.)*. I provided a report explaining basic data protection concepts and consumer expectations.

2024 Independent expert witness appointed by the court in *Czarnionka v. The Epoch Times Association, Inc., No. 1:22-cv-6348 (S.D.N.Y.)*. I was asked to perform a technical analysis to confirm that the terms of the injunctive relief were being followed.

2023-2024 Expert witness for the plaintiffs in *Frasco v. Flo Health, et al., No. 3:21-cv-00757 (N.D. Cal.)*. I provided an expert report based on my forensic analysis of a mobile app's data collection behaviors (i.e., privacy analysis). I was deposed and also provided rebuttal reports of opposing experts.

2023 Expert witness for the California Department of Justice in *NetChoice, LLC v. Bonta, No. 5:22-cv-08861*. I provided a declaration opposing the motion to dismiss.

2022 Expert witness for the plaintiffs in *Hart, et al. v. TWC Product and Technology LLC, No. 4:20-cv-3842-JST*. I provided a rebuttal report and was deposed by opposing counsel.

2022 Expert witness for the District of Columbia Office of the Attorney General in *District of Columbia v. Town Sports International LLC*. I provided a rebuttal report on proper surveying methodology and was deposed by opposing counsel.

2021 Expert witness testifying before the U.S. Senate (Committee on Commerce, Science, and Transportation), hearing on "Protecting Kids Online: Internet Privacy and Manipulative Marketing." Testimony available at: https://www.commerce.senate.gov/2021/5/protecting-kids-online-internet-privacy-and-manipulative-marketing

2017-2019 Expert witness for the plaintiffs in *Vizio, Inc., Consumer Privacy Litigation, No. 8:16-ml-02693-JLS-KES*, assisting with discovery strategy and providing explanations of relevant privacy research on users' willingness to pay for privacy in order to assist in quantifying damages.

2016 Expert witness for the FTC in *FTC v. Amazon.com, Inc., No. C14-1028-JCC*, providing testimony on human-computer interaction (HCI) evaluation methods and critiquing opposing expert's report.

2014-2015 Expert witness for the plaintiffs in *Doe vs. Twitter, Inc., No. CGC-10-503630*, providing explanations of relevant privacy research on users' willingness to pay for privacy in order to assist in quantifying damages.

2014 Expert witness for the plaintiffs in *Levy v. Universal Parking of Florida, LLC No. 13-cv-22122 (S.D. Fla.)*, providing written testimony on basic human-computer interaction concepts as they relate to smartphone usage.

2013 Expert witness for the plaintiffs in *LinkedIn User Privacy Litigation, No. 12-cv-03088-EJD (N.D. Cal.)*, providing explanations of information security concepts and providing original research on users' privacy expectations in order to demonstrate and quantify damages.

2012 Expert witness for the plaintiffs in *Netflix Privacy Litigation, No. 5:11-cv-00379-EJD (N.D. Cal.)*, providing explanations of relevant privacy research and the economics of information privacy in order to quantify damages.

grants awarded

2023–2026 **NSA: Improving Security and Safety of Neural Networks through Robust Training, Noise Augmentation, and Safety Metrics (H98230-23-C-0275)** $750,000
Co-PI (PI: Michael Mahoney, International Computer Science Institute)

2023–2026 **NSF: Measuring, Validating and Improving upon App-Based Privacy Nutrition Labels (CNS-2247951/2247952/2247953)** $600,000
Principal Investigator (Collaborative with Adam Aviv, George Washington University; Chris Kanich, University of Illinois at Chicago)

2022–2025 **NSF: Developer Implementation of Privacy in Software Systems (CCF-2217771/2217772)** $750,000
Principal Investigator (Collaborative with Primal Wijesekera, International Computer Science Institute; Jon Atwell and Julian Nyarko, Stanford University)

2022–2026 **KACST-UCB Center of Excellence for Secure Computing** $6,460,000
Senior Personnel (PI: David Wagner, University of California, Berkeley)

2021–2022 **CITRIS: Auditing the Compliance of California Consumer Privacy Regulations at Scale** $60,000
Principal Investigator (Collaborative with Zubair Shafiq, University of California, Davis)

2019 **Google: ASPIRE: SDK Traffic Identification at Scale** $75,000
Principal Investigator

2018-2022 **NSF: Mobile Dynamic Privacy and Security Analysis at Scale (CNS-1817248)** $668,475
Principal Investigator

2018-2022 **NSF: Contextual Integrity: From Theory to Practice (CNS-1801501/1801307/1801316)** $1,199,462
Principal Investigator (Collaborative with Helen Nissenbaum, Cornell University; and Norman Sadeh, Carnegie Mellon University)

2018-2022	**NSF: Increasing Users' Cyber-Security Compliance by Reducing Present Bias (CNS-1817249)** Principal Investigator	$558,018
2018-2023	**NSA: The Science of Privacy: Implications for Data Usage (H98230-18-D-0006)** Principal Investigator (Co-PI: Michael Tschantz, International Computer Science Institute)	$3,236,424
2018-2019	**DHS: Scaling Contextual Privacy to MDM Environments (FA8750-18-2-0096)** Principal Investigator	$480,000
2018-2019	**Rose Foundation: AppCensus: Mobile App Privacy Analysis at Scale** Principal Investigator (Co-PI: Irwin Reyes, International Computer Science Institute)	$40,000
2018	**Cisco: Access Controls for an IoT World** Principal Investigator	$99,304
2018	**CLTC: Privacy Analysis at Scale** Principal Investigator	$50,000
2018	**CLTC: Secure Internet of Things for Senior Users** Co-PI (PI: Alisa Frik, International Computer Science Institute)	$60,590
2017	**Mozilla: Towards Usable IoT Access Controls in the Home** Principal Investigator	$46,000
2017	**Data Transparency Lab (DTL) / AT&T: Transparency via Automated Dynamic Analysis at Scale** Principal Investigator	$55,865
2017	**CLTC: Secure & Usable Backup Authentication** Co-PI (PI: David Wagner, University of California, Berkeley)	$48,400
2016 - 2017	**NSF: Teaching Security in CSP (CNS-1636590)** Co-PI (PI: Julia Bernd, ICSI)	$200,000
2016 - 2017	**DHS: A Platform for Contextual Mobile Privacy (FA8750-16-C-0140)** Principal Investigator	$664,378
2016 - 2018	**CLTC: The Security Behavior Observatory** Principal Investigator	$195,962
2016	**CLTC: Using Individual Differences to Tailor Security Mitigations** Principal Investigator	$100,000
2015 - 2018	**NSF/BSF: Using Individual Differences to Personalize Security Mitigations (CNS-1528070/BSF-2014626)** Principal Investigator (Collaborative with Eyal Peer, Bar-Ilan University)	$724,732
2015 - 2019	**NSF: Security and Privacy for Wearable and Continuous Sensing Platforms (CNS-1514211/1514457/1513584)** Principal Investigator (Collaborative with David Wagner, University of California, Berkeley; and Franziska Roesner, University of Washington)	$1,200,000
2014 - 2016	**NSF: Teachers' Resources for Online Privacy Education (DGE-1419319)** Co-PI (PI: Gerald Friedland, ICSI)	$300,000
2014 - 2017	**NSA: User Security Behavior** Subcontract (PIs: Lorrie Cranor, Rahul Telang, Alessandro Acquisti, and Nicholas Christin; Carnegie Mellon University)	$200,000
2014	**Google: Improving Security Warnings by Examining User Intent** Principal Investigator	$71,500

2013 - 2015 **NSF: Designing Individualized Privacy and Security Systems (CNS-1343433/1343451)** $132,620
Principal Investigator (Collaborative with Eyal Peer, Carnegie Mellon University)

2013 - 2016 **NSF: A Choice Architecture for Mobile Privacy and Security (CNS-1318680)** $500,000
Co-PI (PI: David Wagner, University of California, Berkeley)

2010 **Google: Designing Usable Certificate Dialogs in Chrome** $60,000
Principal Investigator

patents awarded

2023 Automatic identification of applications that circumvent permissions and/or obfuscate data flows (US Patent 11,689,551)

professional activities

program committees

2023 Privacy Enhancing Technologies Symposium (PETS); IEEE Security & Privacy; Workshop on Economics and Information Security (WEIS)

2022 Contextual Integrity (CI) Symposium

2021 Workshop on Economics and Information Security (WEIS)

2020 ACM CCS; Workshop on Economics and Information Security (WEIS); Symposium on Usable Privacy and Security (SOUPS); USENIX Security

2019 Privacy Enhancing Technologies Symposium (PETS); Workshop on Economics and Information Security (WEIS); Symposium on Usable Privacy and Security (SOUPS)

2018 ACM SIGCHI (Human Factors in Computing Systems); Privacy Enhancing Technologies Symposium (PETS); Workshop on Economics and Information Security (WEIS); ACM Conference on Computer and Communications Security (CCS); Symposium on Usable Privacy and Security (SOUPS); IEEE Security & Privacy ("Oakland")

2017 ACM SIGCHI (Human Factors in Computing Systems); USENIX Security; Privacy Enhancing Technologies Symposium (PETS); New Security Paradigms Workshop (NSPW), **Co-Chair**; Workshop on Economics and Information Security (WEIS); ACM Conference on Computer and Communications Security (CCS); Symposium on Usable Privacy and Security (SOUPS)

2016 Workshop on the Economics of Information Security (WEIS), **Chair**; New Security Paradigms Workshop (NSPW), **Co-Chair**; ACM SIGCHI (Human Factors in Computing Systems); USENIX Security; Symposium on Usable Privacy and Security (SOUPS); ACM WWW; Financial Cryptography and Data Security; Privacy Enhancing Technologies Symposium (PETS)

2015 Symposium on Usable Privacy and Security (SOUPS); USENIX Security; ACM SIGCHI (Human Factors in Computing Systems); Privacy Enhancing Technologies Symposium (PETS); Workshop on the Economics of Information Security (WEIS); ACM WWW; Financial Cryptography and Data Security

2014 ACM SIGCHI (Human Factors in Computing Systems); Financial Cryptography and Data Security; ACM WWW; Privacy Enhancing Technologies Symposium (PETS)

2013 ACM SIGCHI (Human Factors in Computing Systems); Symposium on Usable Privacy and Security (SOUPS); New Security Paradigms Workshop (NSPW); Anti-Phishing Working Group eCrime Researchers Summit

2012 Symposium on Usable Privacy and Security (SOUPS); New Security Paradigms Workshop (NSPW)

2011	Symposium On Usable Privacy and Security (SOUPS); New Security Paradigms Workshop (NSPW); Computers, Freedom, and Privacy (CFP) Conference (poster session co-chair); Software and Usable Security Aligned for Good Engineering (SAUSAGE) Workshop, **Co-Chair**
2010	Symposium On Usable Privacy and Security (SOUPS)
2008	Conference on Information and Knowledge Management (CIKM)
2007	ACM SIGCHI Workshop - Security User Studies: Methodologies and Best Practices; Anti-Phishing Working Group eCrime Researchers Summit (poster session co-chair)
2006	Computers, Freedom, and Privacy (CFP) Conference

standards committees

2007-2008	W3C Web Security Context (WSC) Working Group
2004-2006	W3C Platform for Privacy Preferences (P3P) 1.1 Working Group

leadership roles

2012-Now	Director, Berkeley Laboratory for Usable and Experimental Security (BLUES)
2021-2023	Member, ICSI Scientific Leadership Council
2006-2008	Legislative Concerns Chair / Board of Directors, National Association of Graduate and Professional Students (NAGPS)
2006-2008	Vice President for External Affairs, Carnegie Mellon Graduate Student Assembly

teaching

Fall 2019 — **Usable Privacy and Security** — University of California, Berkeley
Designed and taught a course as part of the School of Information's Masters in Cybersecurity program. Duties included course design and development, grading assignment and exams, supervising class projects, and holding office hours.

Spring 2017, Spring 2018 — **Human Factors in Computer Security and Privacy** — Brown University
Instructor for a module on "user interfaces for security" as part of the Executive Masters in Cybersecurity program. Duties included course design and development, grading assignments and exams, supervising thesis projects, and holding office hours.

Fall 2007 — **Information Security & Privacy (46-861)** — Carnegie Mellon University
Teaching assistant duties included developing course materials (topics for lectures, assignments, and exams), grading assignments and exams, holding office hours, and mentoring students about semester-long projects.

Spring 2006 — **Computers and Society (15-290)** — Carnegie Mellon University
Teaching assistant duties included giving guest lectures, creating assignments and exams, grading assignments and exams, holding office hours, and mentoring students about semester-long projects.

Fall 2003 — **Information Security (CS 451)** — University of Virginia
Teaching assistant duties included giving guest lectures, creating assignments and exams, grading assignments and exams, and holding office hours.

Fall 2003 — **Intellectual Property (TCC 200)** — University of Virginia
Teaching assistant duties included grading assignments and holding office hours.

Spring 2003, Spring 2004 — **Advanced Software Development Methods (CS 340)** — University of Virginia
Teaching assistant duties included grading and holding office hours.

Fall 2002 — **Engineering Software (CS 201J)** — University of Virginia
Teaching assistant duties included grading assignments and holding office hours.